REMARKS

This Amendment is in response to the Office Action mailed June 11, 2007. Claims 1-26 are pending. Claims 10-12 and 24-26 have been allowed. Claims 5, 6, 15-17, 20, and 21 have been objected to. In this response, claims 1, 3, 4, 10, and 24 have been amended. No claims have been added or canceled. Reconsideration in light of the amendments and remarks made herein is respectfully requested.

Applicants wish to thank the Examiner for the thorough examination, and for holding some of the claims allowable.

Applicants are resubmitting an Information Disclosure Statement (IDS) including two references originally submitted by the Applicants in an IDS on April 1, 2004, and six references originally submitted by the Applicants in an IDS on June 23, 2004. However, because the Examiner only initialed the first page of the April 1, 2004 IDS and did not respond to the June 23, 2004 IDS, Applicants are resubmitting the references to ensure that the Examiner has them available. Applicants respectfully request that the Examiner consider these references and initial the enclosed 1449 form.

Rejection Under 35 U.S.C. § 112

The Examiner rejects claims 3-5, 10-12 and 24-26 under 35 U.S.C. § 112, second paragraph, as being indefinite. With respect to claims 3, 4, and 24, the Examiner noted that the claims lacked a sufficient antecedent basis for certain limitations within those claims. Applicants have amended the claims as suggested by the Examiner, and respectfully request withdrawal of the rejections of claims 3, 4, and 24, and the claims that depend therefrom.

With respect to claim 10, the Examiner stated that it "is unclear to the Examiner as to which entity is receiving the request for a certificate" and "which entity is forwarding the

request" (Office Action, mailed 6/11/2007, pages 2-3). Applicants have accordingly amended the claims to clarify which entity is receiving and forwarding the request, as requested by the Examiner. In light of the amendments, Applicants respectfully request the withdrawal of the rejection of claim 10 under § 112, and the claims that depend therefrom.

With respect to claim 24, the Examiner stated it is unclear "how the engine uses a private key as a virtual smart card" (Office Action, mailed 6/11/2007, page 3). Under MPEP § 2173.01 a "fundamental principle contained in 35 U.S.C. 112, second paragraph is that applicants are their own lexicographers. They can define in the claims what they regard as their invention essentially in whatever terms they choose so long as any special meaning assigned to a term is clearly set forth in the specification." Based on the principle that the Applicants may use and describe their own claim terminology, Applicants respectfully draw the Examiner's attention to the Applicants' specification. In particular, the Applicants recite:

> Client II 160 illustrates the same user roaming, i.e. on a different computer system, connecting to a server 130 through the network 140. Client II 160 does not have the user's private key or certificate. Therefore, the user has to carry a smart card or diskette 170 on which the user's certificate and private key are stored. Again, the certificate and private key may be protected by a password. However, smart cards can be lost, and require a user to remember to carry something.
> (Specification, page 2, lines 5-10)

The cited paragraph describes a traditional smartcard, which was used to physically carry encryption keys, while providing a portable means of supplying user data for encryption purposes. Applicants' claim 24, however, recites limitations which provide for portable encryption solutions that use a user's private key received over network, without the requirement that a traditional/physical smartcard be utilized. Thus, Applicants respectfully submit that claim 24, which recites in part "a cryptographic engine to use a user's private key, as a virtual smart

card, to perform the requested cryptographic function after the user has been authenticated by the authentication engine," is clear in light of the Specification and as would be understood by one of ordinary skill in the art. Therefore, Applicants request the rejection of claim 24 under § 112, and the claims that depend therefrom, be withdraw.

Applicants respectfully request that the Examiner withdraw the rejection of claims 3-5, 10-12 and 24-26 under 35 U.S.C. § 112, second paragraph.

Rejection Under 35 U.S.C. § 103

The Examiner rejects claims 1-3, 7-9, and 22-23 under 35 U.S.C. § 103(a) as being unpatentable over Hoffman, et al. (U.S. Patent No. 6,012,039) in view of Ganesan (U.S. Patent No. 5,535,276). Applicants respectfully disagree.

Hoffman describes a reward authorization system between an issuer and a recipient, in which recipient biometric data is utilized (Hoffman, Abstract). A server stores pre-verified recipient biometric data (Hoffman, column 6, line 66 to column 7, line 8). When a recipient makes a bid for a reward, they provide a sample of biometric data, and both the bid and the associated biometric data are transmitted to the server. The server then verifies a match between the submitted biometric data and the sample biometric data (Hoffman, column 10, lines 1-21).

Ganesan describes a system of providing a secure communication connection (Ganesan, Abstract; column 8, lines 9-43). The connection is secured when a first user generates a temporary key pair, on the user's computer, to encrypt a message and exchange the pair and message with a server (Ganesan, column 8, lines 20-25). This method allows another user to then further encrypt a message when the user generates their own temporary key pair to identify each other through the server. Thus, in each case, the temporary key pairs are generated by a

communication initiator, and in response to initiating a communication (*See* Ganesan, column 8, lines 40-44; column 9, lines 17-54).

Claim 1 recites:

> A method of providing remote cryptographic services, the method comprising at a biometric certification server (BCS):
> establishing a secure connection between a client and the biometric certification server (BCS);
> receiving a request for a cryptographic service from the client;
> receiving biometric data from a user;
> the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data; and
> the BCS performing the requested cryptographic service.
>
> (Emphasis Added)

That is, in accordance with claim 1, a server generates a disposable public key/private key pair after user authentication, such that the user is not required to create the disposable key pair. Applicants respectfully submit that neither Hoffman nor Ganesan, alone or in combination, teaches or suggests "the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data."

The Examiner stated that Hoffman fails to teach "generating a disposable public key/private key pair" (Office Action, mailed 6/11/2007). The Examiner stated, however, that Hoffman performs a cryptographic service if the user is authenticated based on the biometric data (Office Action, mailed, 6/11/2007 *citing* Hoffman, column 9, line 44 to column 10, line 32). However, Hoffman merely describes receiving a biometric sample, attempting to match the biometric sample to biometric data already stored in a database, and sending a message as to whether the authentication was successful (Hoffman, column 10, lines 1-32). Thus, Hoffman merely performs a database search in response to receiving a recipient's biometric data sample, but fails to teach or suggest performing any

cryptographic services after a user is authenticated based on biometric data. Therefore, Hoffman must fail to teach or suggest "the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data."

Furthermore, as discussed above, temporary key pairs are generated in Ganesan by communication initiators. There is no discussion or hint within Ganesan that a server generates a disposable public key/private key pair *after* user authentication. Therefore, Ganesan also fails to teach or suggest performing any cryptographic services after a user is authenticated based on biometric data, and thus fails to teach or suggest "the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data."

Therefore, Applicants respectfully submit that claim 1 is not rendered obvious under 35 U.S.C. § 103 over Hoffman in view of Ganesan. Furthermore, dependent claims 2-3 and 7-9, which depend from claim 1 are also not rendered obvious under 35 U.S.C. § 103.

With respect to independent claim 22, the applicants claim "the remote crypto-server to generate a disposable public key/private key pair and perform the requested cryptographic function when the user is successfully authenticated using the biometric data." Similar to the discussion above, neither Hoffman nor Ganesan describe or suggest a remote crypto-server to generate a public key/private key pair when a user is authenticated using biometric data. Therefore, claim 22 is not rendered obvious under 35 U.S.C. § 103 over Hoffman in view of Ganesan.

With respect to independent claim 23, the applicants claim a crypto server that generates a disposable public key/private key pair and performs a cryptographic function, where the crypto

server further authenticates a user based on biometric data. For reasons similar to the discussion above, neither Hoffman nor Ganesan describe or suggest the crypto server to generate a disposable public key/private key pair as claimed in claim 23. Therefore, claim 23 is also not rendered obvious under 35 U.S.C. § 103 over Hoffman in view of Ganesan.

Applicants respectfully request that the Examiner withdraw the rejection of claims 1-3, 7-9, and 22-23 under 35 U.S.C. § 103(a) as being unpatentable over Hoffman in view of Ganesan.

The Examiner rejects claims 13-21 under 35 U.S.C. § 103(a) as being unpatentable over Hoffman in view of Jakobsson (U.S. Patent No. 6,587,946). Applicants respectfully disagree.

Claim 13, as amended, claims:

> An apparatus for performing remote cryptographic functions comprising:
> a crypto-server having a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;
> an authentication engine for authenticating the user based on biometric data received through the crypto-proxy interface of the crypto-server;
> a cryptographic engine for performing the cryptographic functions after the authentication engine has authenticated the user based on the biometric data; and
> the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.
>
> (Emphasis Added)

The Applicants respectfully submit that claim 13 is not rendered obvious by Hoffman in view of Jakobsson.

As discussed above, Hoffman describes a method that utilizes a biometric sample to authenticate a user in a transaction. A biometric data sample is transmitted to a system which attempts to locate or verify a match to an existing biometric sample (Hoffman, column 9, line 44 to column 10, line 32). However, Hoffman merely matches a biometric data sample with pre-

stored samples Hoffman, and fails to teach or suggest performing any cryptographic services after a user is authenticated based on biometric data.

Jakobsson describes a system for providing an encrypted message to a second recipient when the primary recipient is unavailable (Jakobsson, Column 3, lines 9-15; Column 5, lines 1-47). In the system, portions of the primary recipient's private encryption key are shared among a quorum of proxy servers (Jakobsson, Column 3, lines 37-41; Column 7, lines 25-28). Each of the proxy servers modifies the message so that it can be delivered to a secondary recipient such that the secondary recipient can decipher the message (Jakobsson, Abstract). However, Jakobsson fails to discuss the use of biometric data in the messaging system.

The Applicants, however, claim a crypto-server having a crypto-proxy interface that receives requests for cryptographic functions, receives biometric data, and returns data to a client after the cryptographic function has been performed. Further, the cryptographic function is performed after a user has been authenticated by an authentication engine of the crypto-server. As discussed above, Hoffman fails to teach or suggest performing any cryptographic functions after a user has been authenticated based on biometric data. Furthermore, as discussed above, the messaging system described in Jakobsson fails to teach or suggest the use of biometric data in messaging process or the messaging proxy servers. Thus, Jakobsson also fails to teach or suggest a crypto-server for receiving requests, receiving biometric data, and returning data after the requested cryptographic function is performed and the user is authenticated. Therefore, neither Hoffman nor Jakobsson, teaches or suggests a crypto-server having a crypto-proxy interface that receives requests for cryptographic functions, receives biometric data, and returns data to a client after the cryptographic function has been performed and the biometric data of the user has been authenticated.

Therefore, since neither Hoffman nor Jakobsson teach or suggest each and every element as claimed in claim 13, claim 13 and the claims that depend therefrom are not rendered obvious by Hoffman in view of Jakobsson. Applicants respectfully request that the Examiner withdraw the rejection of claims 13-21 under 35 U.S.C. § 103(a) as being unpatentable over Hoffman in view of Jakobsson.

Allowable Subject Matter

Applicants note with appreciation the Examiner's allowance of claims 10-12 and 24-26. Applicants further note with appreciation the Examiner's indication of allowable subject matter, as claimed in claims 4-6, 15-17 and 20-21.

Conclusion

Applicant reserves all rights with respect to the applicability of the doctrine of equivalents. Applicant respectfully requests that a timely Notice of Allowance be issued in this case. If a telephone interview would expedite the prosecution of this application, the Examiner is invited to contact William L. Jaffe at (714) 557-3800.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: By_____
William W. Schaal
Reg. No. 39,018
Tel.: (714) 557-3800 (Pacific Coast)

CERTIFICATE OF MAILING/TRANSMISSION (37 CFR 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

☐ *deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, PO Box 1450, Alexandria, VA 22313-1450.*

Date: December 11, 2007

FACSIMILE

☒ *transmitted by facsimile to the Patent and Trademark Office.*

Susan McFarlane December 11, 2007
Date